PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-347944
(43)Date of publication of application : 15.12.2000

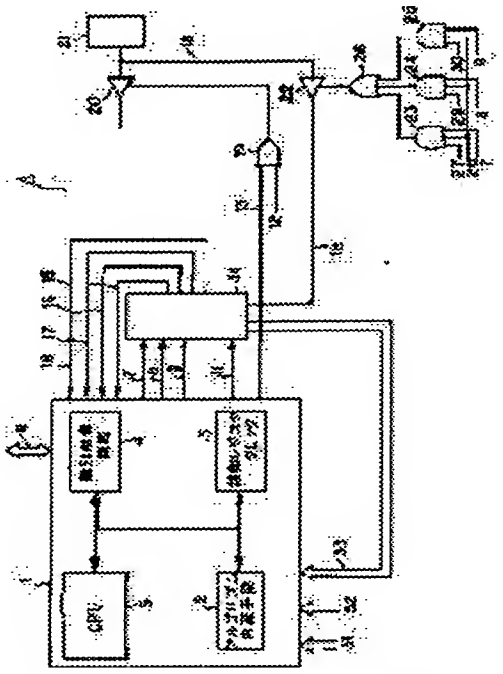
(51)Int.Cl. G06F 12/14

(21)Application number : 11-159486
(22)Date of filing : 07.06.1999

(71)Applicant : SHARP CORP
(72)Inventor : HAYASHI HIROTAKE

(54) MICROCOMPUTER WITH BUILT-IN NONVOLATILE MEMORY

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a one-chip microcomputer with a built-in nonvolatile memory capable of performing security protection of data with a simple operation.
SOLUTION: This microcomputer is provided with a dedicated security flash memory 14 which automatically stores the last data to be written in an internal flash memory 21 as a security code, a controller 1 controlling an access to the memory 21, an OR circuit 19 and a tri-state buffer 20. After the data writing to the memory 21 is finished, the controller 1, etc., is allowed to access the memory 21 only when data coinciding with a security code is inputted externally.



LEGAL STATUS

[Date of request for examination] 18.01.2002
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

引用例３の写し

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－347944
（P2000－347944A）
(43)公開日　平成12年12月15日(2000.12.15)

(51)Int.Cl.'	識別記号	Ｆ Ｉ	テーマコード'（参考）
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｃ　５Ｂ０１７

審査請求　未請求　請求項の数６　ＯＬ　（全７頁）

(21)出願番号　特願平11－159486

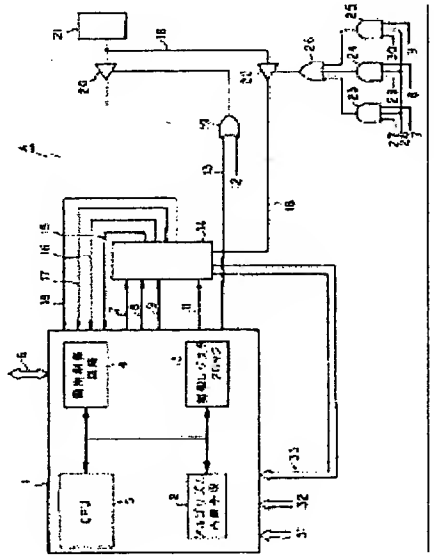
(22)出願日　平成11年６月７日(1999.6.7)

(71)出願人　000005049
シャープ株式会社
大阪府大阪市阿倍野区長池町22番22号
(72)発明者　林　裕▲之▼
大阪府大阪市阿倍野区長池町22番22号　シャープ株式会社内
(74)代理人　100112335
弁理士　藤本　英介

Ｆターム(参考)　5B017 AA01 BA05 CA13

(54)【発明の名称】　不揮発性メモリ内蔵マイクロコンピュータ

(57)【要約】
【課題】　簡単な操作によってデータの機密保持が可能な不揮発性メモリ内蔵１チップマイクロコンピュータを提供すること。
【解決手段】　内蔵フラッシュメモリ２１へ書き込まれる最終データをセキュリティコードとして自動的に記憶するセキュリティ専用フラッシュメモリ１４と、内蔵フラッシュメモリ２１へのアクセスを制御する制御装置１、ＯＲ回路１９、およびトライステートバッファ２０とを設け、制御装置１等は、内蔵フラッシュメモリ２１へのデータの書き込み終了後においては、セキュリティコードと一致するデータが外部から入力された場合にのみ内蔵フラッシュメモリ２１へのアクセスを可能とする。



【特許請求の範囲】
【請求項 1】　不揮発性メモリを内蔵 したマイクロコンピュータであ って、
前記不揮発性メモリへ書き込まれるデータの一部をセキュリティコードとして自動的に記憶するセキュリティ専用不揮発性メモリと、
前記不揮発性メモリへのアクセスを制御する制御手段とを設け、
前記制御手段は、前記不揮発性メモリへのデータの書き込み終了後においては、前記セキュリティコードと一致するデータが外部から入力された場合に不揮発性メモリへのアクセスを可能とすることを特徴とする不揮発性メモリ内蔵 マイクロコンピュータ。
【請求項 2】　不揮発性メモリを内蔵 したマイクロコンピュータであ って、
前記不揮発性メモリへ書き込まれるデータの一部をセキュリティコードとして自動的に記憶するセキュリティ専用不揮発性メモリと、
前記不揮発性メモリに対するアクセスを制御するアルゴリズム を内蔵 したアルゴリズム 内蔵 手段と、
前記セキュリティ専用不揮発性メモリへのセキュリティコードの記憶終了後に、前記アルゴリズム 内蔵 手段の制御の下で、前記不揮発性メモリへのアクセスを禁止するアクセス禁止手段と、を設けたことを特徴とする不揮発性メモリ内蔵 マイクロコンピュータ。
【請求項 3】　前記アクセス禁止手段は、前記アルゴリズム 内蔵 手段に格納されたアルゴリズム で無限ループを実行することで不揮発性メモリへのアクセスを禁止することを特徴とする請求項 2に記載の不揮発性メモリ内蔵 マイクロコンピュータ。
【請求項 4】　前記セキュリティコードと一致するデータを外部より入力することにより、前記アクセス禁止手段による不揮発性メモリへのアクセス禁止状態を解除することを特徴とする請求項 2又は3に記載の不揮発性メモリ内蔵 マイクロコンピュータ。
【請求項 5】　不揮発性メモリへのアクセスを可能、或いは不揮発性メモリへのアクセス禁止状態を解除した後に、セキュリティコードと一致しないデータを外部より入力することにより再度不揮発性メモリへのアクセスを禁止することを特徴とする請求項 1又は4に記載の不揮発性メモリ内蔵 マイクロコンピュータ。
【請求項 6】　前記セキュリティコードは、不揮発性メモリへ書き込まれる最終データであ ることを特徴とする請求項 1又は2に記載の不揮発性メモリ内蔵 マイクロコンピュータ。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、マイクロコンピュータに内蔵 される不揮発性メモリのメモリデータを読み出し装置から読み出し不可能とするようなメモリデータ保護に関する。
【０００２】
【従来の技術】従来、不揮発性メモリ（例えばフラッシュメモリー）の内蔵 された１チップマイクロコンピュータでは、内蔵 不揮発性メモリへのアクセス、すなわちデータ書き込み、読み出し、データ消去を行う際、後述の3種の動作モードが用意され、各モード毎に専用ボードが使用される。これらの動作モードを実現する概略的な構成は内蔵 不揮発性メモリにアクセスするアルゴリズムを内蔵 している不揮発性のプログラム メモリ、ＣＰＵ及び内蔵 不揮発性メモリアクセス動作に関連する識別制御回路、制御レジスタ等からなる。
【０００３】これらのモードには、（１）ＰＲＯＭライターによる専用アダプタを使用しデータの書き込み、消去、読み出しの行えるＰＲＯＭモード、（２）外部メモリ（ＰＲＯＭ等）から専用ボードを使用してフラッシュメモリへデータのコピーを行うコピーモード、（３）製品のプリント基板に実装されたフラッシュメモリーの内蔵 された１チップマイクロコンピュータデバイスに対してシリアルポートを介してデータを書き込むシリアル転送モード（以下、オンボードモードという）があ る。そこで、これらの各モードでメモリデータの機密保持を行う必要があ る場合、それを実現するための機能を各モード毎に備えていなければならない。
【０００４】従来、本機能を実現するために以下のようなものがあ る。
（ａ）ＰＲＯＭライタによるデータの読み出しを行う際、予め入力されたセキュリティコードが不揮発性メモリへ記憶されており、このセキュリティコードに対するコードを外部端子等で入力し、一致しない限り読み出し禁止とする。あ るいは、書き込みを行う際、特定の端子等を設定することで、ＰＲＯＭライタでの再度の書き込み及び読み出しを不可能とする。このようにして、メモリデータ機密保持を図る。
【０００５】（ｂ）コピーモードによる書き込みも前記（ａ）同様予め入力されたセキュリティコードが不揮発性メモリへ記憶されおり、このセキュリティコードに対するコードを外部端子等で入力し一致しない限り読み出しが禁止になりメモリデータの保護が行われる。
【０００６】（Ｃ）オンボードモードでは、所定のフォーマットに従ってプログラム にパスワードを予め設定しユーザプログラム 書き込み時に同一のパスワードを入力しない限りアクセスされないことで保護される。
【０００７】上記のように本来のデータアクセス以外に予め、セキュリティコードあ るいはパスワードを設定する必要があ る。
【０００８】図２に、従来技術の一例による不揮発性メモリを内蔵 した１チップマイクロコンピュータのデータメモリ保護に対する概略的な構成例を示す。これは、特開平５－７３４２８に開示されている技術を簡略に示し

たものである。不揮発性メモリが内蔵されたメモリデータを読み出し禁止とする方法として、セキュリティコード記憶不揮発性メモリ１００へ予めコードを記憶させ、入力キーコードラッチ回路１０１でセキュリティコード記憶不揮発性メモリ１００へ記憶させたコードと同一コードを入力する。この情報は比較回路１０２で判断され一致している場合のみ読み出し制御部１０３へ一致信号が出力されて、比較結果用不揮発性メモリ１０４からの比較結果信号１０５と、図示しないＣＰＵからのリード信号１０６とでメモリ１０８を読み出し可能とする。イネーブル信号１０７が出力されることで、メモリ１０８から図示しない内部データバス或いは、外部の端子へデータの読み出しが行われる。

【０００９】

【発明が解決しようとする課題】しかしながら、従来の方法では予めセキュリティコードを不揮発性メモリへ設定し、このセキュリテコードに対するコードを外部より入力しなければならず、メモリデータへの書き込みを行う操作以外の設定による作業が必要になると同時に、セキュリテコードを改めて規定するためにその管理が煩雑となっていた。

【００１０】本発明は、前記の問題点を解消するためなされたものであって、簡単な操作によってデータの機密保持が可能な不揮発性メモリ内蔵１チップマイクロコンピュータを提供することを目的とする。

【００１１】

【課題を解決するための手段】本発明は、上記の目的を達成するため、次の構成を有する。本発明の第１の要旨は、不揮発性メモリを内蔵したマイクロコンピュータであって、前記不揮発性メモリへ書き込まれるデータの一部をセキュリティコードとして自動的に記憶するセキュリティ専用不揮発性メモリと、前記不揮発性メモリへのアクセスを制御する制御手段とを設け、前記制御手段は、前記不揮発性メモリへのデータの書き込み終了後においては、前記セキュリティコードと一致するデータが外部から入力された場合に不揮発性メモリへのアクセスを可能とすることを特徴とする不揮発性メモリ内蔵マイクロコンピュータである。

【００１２】また、本発明の第２の要旨は、不揮発性メモリを内蔵したマイクロコンピュータであって、前記不揮発性メモリへ書き込まれるデータの一部をセキュリティコードとして自動的に記憶するセキュリティ専用不揮発性メモリと、前記不揮発性メモリに対するアクセスを制御するアルゴリズム を内蔵したアルゴリズム 内蔵 手段と、前記セキュリティ専用不揮発性メモリへのセキュリティコードの記憶終了後に、前記アルゴリズム 内蔵 手段の制御の下で、前記不揮発性メモリへのアクセスを禁止するアクセス禁止手段と、を設けたことを特徴とする不揮発性メモリ内蔵マイクロコンピュータである。

【００１３】さらに、本発明の第３の要旨は、前記アクセス禁止手段は、前記アルゴリズム 内蔵 手段に格納されたアルゴリズム で無限ループを実行することで不揮発性メモリへのアクセスを禁止することを特徴とする要旨２に記載の不揮発性メモリ内蔵マイクロコンピュータである。

【００１４】また、本発明の第４の要旨は、前記セキュリティコードと一致するデータを外部より入力することにより、前記アクセス禁止手段による不揮発性メモリへのアクセス禁止状態を解除することを特徴とする要旨２又は３に記載の不揮発性メモリ内蔵マイクロコンピュータである。

【００１５】また、本発明の第５の要旨は、不揮発性メモリへのアクセスを可能、或いは不揮発性メモリへのアクセス禁止状態を解除とした後に、セキュリティコードと一致しないデータを外部より入力することにより再度不揮発性メモリへのアクセスを禁止することを特徴とする要旨１又は４に記載の不揮発性メモリ内蔵マイクロコンピュータである。

【００１６】さらにまた、本発明の第６の要旨は、前記セキュリティコードは、不揮発性メモリへ書き込まれる最終データであることを特徴とする要旨１又は２に記載の不揮発性メモリ内蔵マイクロコンピュータである。

【００１７】要旨１によれば、不揮発性メモリへデータが書き込まれると同時、或いは書き込まれた後に、セキュリティ専用不揮発性メモリにそのデータの一部がセキュリティコードとして自動的に記憶される。セキュリティコードは所定ルールに基づきくものであるので、データを書き込んだ者は知り得るが、他人には知れ得ないこととなる。そして、その不揮発性メモリへのデータへの書き込みが終了した後には、セキュリティコードと一致するデータが外部から入力されないかぎり、制御手段が不揮発性メモリへの再度のアクセスを不可とするので、他人による書き込み動作、読み出し動作、消去動作等のアクセスが不可となり、不揮発性メモリ内のデータの機密保持が可能となる。従来、不揮発性メモリ内のデータの機密保持を行なう場合には、不揮発性メモリへデータの書き込み操作と別個にセキュリティコードの入力操作を行なっていたが、本発明ではセキュリティコードの入力操作が不要となるのと同時に、改めてセキュリティコードを用意する必要もなくなるので簡単な手段にて機密保持が可能となった。

【００１８】また、要旨２によれば、不揮発性メモリへデータが書き込まれると同時、或いは書き込まれた後に、セキュリティ専用不揮発性メモリにそのデータの一部がセキュリティコードとして自動的に記憶される。そして、セキュリティ専用不揮発性メモリへのセキュリティコードの記憶終了後は、アルゴリズム 内蔵 手段の制御の下で、アクセス禁止手段が不揮発性メモリへの再度の書き込み動作、読み出し動作、消去動作等のアクセスを禁止するので、他人によるアクセスが不可となり、不揮

発性メモリ内のデータの機密保持が可能となる。従来、不揮発性メモリ内のデータの機密保持を行なう場合には、不揮発性メモリへデータの書き込み操作と別個にセキュリティコードの入力操作を行なっていたが、本発明ではセキュリティコードの入力操作が不要となるのと同時に、改めてセキュリティコードを用意する必要もなくなるので簡単な手段にて機密保持が可能となった。

【００１９】また、要旨３によれば、アクセス禁止手段がアルゴリズム内蔵手段に格納されたアルゴリズムで無限ループを実行することで、アクセス待ち状態（データ書き込み動作、消去動作、読み出し動作のいずれかに相当するルーチン待ち）が無く、見かけ上アクセス不能状態となる。すなわち、デバイス自体が内蔵メモリをアクセスできない故障あるいは不良の状態と同等となるため、実質的に他者によるメモリデータの読み出しは困難でありメモリ内容のセキュリティーが保たれる。

【００２０】さらにまた、要旨４によれば、セキュリティコードは所定ルールに基づくものでありデータを書き込んだ者は知り得るので、不揮発性メモリ内のデータの修正等を行なう場合にはセキュリティコードと一致するデータを外部より入力することにより可能となる。

【００２１】また、要旨５によれば、不揮発性メモリ内のデータの修正等を行った後に、セキュリティコードと一致しないデータを外部より入力するという簡単な操作により再度不揮発性メモリへのアクセスを禁止することが可能となり、簡単な操作により修正が可能となる。

【００２２】さらに、要旨６によれば、セキュリティコードを不揮発性メモリへ書き込まれる最終データとすることで、セキュリティコード等の設定が簡単な回路により実現することができる。

【００２３】

【発明の実施の形態】以下、図面を参照して本発明の実施形態を詳細に説明する。図１は、マイクロコンピュータであって、より具体的にはプロセッサと共にメモリ、例えばフラッシュメモリを１チップに集積、内蔵した１チップマイクロコンピュータＡの主要部位のブロック図を示している。１は内蔵フラッシュメモリ２１へのアクセスを行う制御装置であり、１４は制御装置１から内蔵フラッシュメモリ２１へのアクセスを制御するためのセキュリティ専用フラッシュメモリ１４である。

【００２４】制御装置１には、ＰＲＯＭモード、コピーモード、オンボードモードの各モードを認識し、書き込み動作、読み出し動作、及び消去動作の各プログラムを内蔵しているアルゴリズム内蔵手段２と、そのアルゴリズム内蔵手段２内のプログラムが実行されて内蔵フラッシュメモリ２１をアクセスする際の制御レジスタブロック３と、ＰＲＯＭモード時のＰＲＯＭライタコマンド等に対する識別制御を行う識別制御回路４と、これらの制御をつかさどるＣＰＵ５とを有する概略構成とし、各モードによる動作を可能とする。尚、制御装置１の各種入出力信号については、後述する。

【００２５】内蔵フラッシュメモリ２１には、図示しない各種出力端子との間に制御スイッチであるトライステートバッファ２０が接続され、内蔵フラッシュメモリ２１からのデータ出力がコントロールされるとともに、内蔵フラッシュメモリ２１とセキュリティ専用フラッシュメモリ１４との間にもトライステートバッファ２２が設けられ、セキュリティ専用フラッシュメモリ１４へのデータ出力も制御されている。

【００２６】前記トライステートバッファ２０のオンオフをコントロールするコントロールゲートは、制御装置１等からの信号を入力信号とするＯＲ回路１９の出力端子に接続され、結果的に制御装置１からの信号１３や後述する信号１２によりそのＯＮ／ＯＦＦ制御が成されている。また、トライステートバッファ２２のコントロールゲートには各モード（ＰＲＯＭモード、コピーモード、オンボードモード）毎に対応して設けられたＡＮＤ回路２３、２４、および２５の出力信号を入力信号とするＯＲ回路２６の出力端子が接続され、各モード毎のセキュリティ専用フラッシュメモリ１４へのデータの出力を制御している。

【００２７】次に、各モードによるセキュリティの動作を説明する。まずＰＲＯＭモードの動作時における制御装置１では、ＰＲＯＭライタインターフェイス信号６を介して図示しないＰＲＯＭライタとのアクセスを可能にする数種類の信号が入出力し、識別制御回路部４でＰＲＯＭライタからのコマンド、データ、制御データの認識を行い、データ書き込みコマンドに対する処理が実行される。これにより、内蔵フラッシュメモリ２１へのＰＲＯＭモードでのデータの書き込みがなされる。

【００２８】そして、最終のデータ書き込みサイクル期間、制御装置１よりＰＲＯＭモード書き込み終了信号７にライト信号２８パルス出力に対し、セットアップ、ホールド期間を保持してＨｉｇｈを出力させる。このとき同様に最終のデータ書き込みサイクル期間、ＰＲＯＭモード書き込み終了信号７はＰＲＯＭモード用のＡＮＤ回路２３へも入力される。

【００２９】ＰＲＯＭモード用のＡＮＤ回路２３の残り２入力信号は、ＰＲＯＭモード信号２７とライト信号２８であり、ＰＲＯＭモード信号２７は現在ＰＲＯＭ書き込みモードであるのでＨｉｇｈとなり、またライト信号２８は最終書き込みデータ期間のみＨｉｇｈパルスが有効となる。以上より、ＡＮＤ回路２３はＨｉｇｈを出力する。

【００３０】そしてＰＲＯＭモード用のＡＮＤ回路２３の出力信号は、トライステートバッファ２２のコントロールゲートを制御するＯＲ回路２６へ入力される。尚、前記ＯＲ回路２６は、各モードに対応して３入力信号となっており、残り２入力の信号はコピーモード用のＡＮＤ回路２４の出力信号とオンボードモード用のＡＮＤ回

路２５の出力信号が入力される。
【００３１】現在ＰＲＯＭ書き込みモードの状態であるために、コピーモード用のＡＮＤ回路２４の入力信号であるコピーモード信号２９と、オンボードモード用のＡＮＤ回路２５の入力信号であるオンボードモード信号３０は共に非アクティブであるのでＯＲ回路２６へはＬｏｗ信号が入力される。よって、ＯＲ回路２６の入力は、ＰＲＯＭモード時のＡＮＤ回路２３の出力信号が有効となってトライステートバッファ２２のコントロールゲートへ入力され、最終書き込みデータ期間のみゲートが開き、セキュリティ専用フラッシュメモリ１４へのデータ出力が可能となる。
【００３２】これにより内蔵 フラッシュメモリ２１からの最終書き込みデータ（ここでは、例として８ビット長のデータを示す）をセキュリティ専用フラッシュメモリ１４に、セキュリティコードとして書き込み、ＰＲＯＭモード書き込み終了信号７と共に設定される。
【００３３】そして、セキュリティ専用フラッシュメモリ１４はＰＲＯＭモードに対するセキュリティが設定されたと認識し、ＰＲＯＭモードセキュリティ信号１５を出力し、この信号１５を受けて、制御装置１内にあるアルゴリズム 内蔵 手段２内のプログラム で強制的に無限ループルーチンへ起動を掛ける。この起動により制御装置１より無限ループフラグ信号１３にＬｏｗが出力される。この信号１３は、ＯＲ回路１９へ入力される。また、ＯＲ回路１９による残りの入力信号である実動作モード信号１２は、ユーザプログラム が起動する時の信号であり、このＰＲＯＭモード時にはＬｏｗ信号である。
【００３４】これらのＬｏｗ信号１２、１３が入力されるＯＲ回路１９は、Ｌｏｗ信号が出力されトライステートバッファ２０のコントロールゲートへ入力され、トライステートバッファ２０の出力はこのコントロールゲートへの入力信号がＨｉｇｈの時のみイネーブルとなることからフローティング状態になり、かつ、制御装置１内にあるアルゴリズム 内蔵 手段２内で実行中のプログラムがＰＲＯＭモード動作に対する待機状態でないので、内蔵 フラッシュメモリ２１のデータをＰＲＯＭライタから読み出すことが不可能となると同時にＰＲＯＭライタからの制御そのものも受け付けなくなる。
【００３５】また、このＰＲＯＭモードで書き込まれたメモリ内容は、コピーモードあるいはオンボードモードで読みだそうとしてもＰＲＯＭモードによる無限ループフラグ信号１３を解除しない限り、読み出せない。尚、無限ループフラグ信号１３を解除し、メモリ内容を読みだし可能とする手段については後述する。
【００３６】次に、コピーモード時はＰＲＯＭモード同様、最終のデータ書き込みサイクル期間、制御装置１よりコピーモード書き込み終了信号８にライト信号２８パルス出力に対し、セットアップ、ホールド期間を保持してＨｉｇｈを出力させる。このとき、コピーモード書き込み終了信号８は、ＡＮＤ回路２４へ入力される。残り２入力のコピーモード信号２９は、現在コピーモード書き込みであるのでＨｉｇｈ信号が入力され、ライト信号２８は最終書き込みデータ期間のみＨｉｇｈパルスが有効となり、結果的にＡＮＤ回路２４からＯＲ回路２６へＨｉｇｈが入力される。
【００３７】このＯＲ回路２６の残り２入力の信号は、ＡＮＤ回路２３の出力とＡＮＤ回路２５の出力であるが、ＡＮＤ回路２３の入力にはＰＲＯＭモード信号２７が入力されており、現在コピーモード書き込みの状態であるるため両ＡＮＤ回路の出力信号はＬｏｗとなっている。従って、ＯＲ回路２６の入力はコピーモード時のＡＮＤ回路２４の出力信号が有効となりトライステートバッファ２２のコントロールゲートへ入力されてゲートが開き、データが出力される。これにより内蔵 フラッシュメモリ２１から最終書き込みデータ期間のデータをセキュリティ専用フラッシュメモリ１４に、セキュリティコードとして書き込み、コピーモード書き込み終了信号８と共に設定される。
【００３８】そして、セキュリティ専用フラッシュメモリ１４はコピーモードに対するセキュリティが設定されたと認識し、コピーモードセキュリティ信号１６を出力し、この信号１６を受けて、制御手段内１にあるアルゴリズム 内蔵 手段２内のプログラム で強制的に無限ループルーチンへ起動を掛ける。この起動により制御装置１より無限ループフラグ信号１３にＬｏｗが出力される。この信号１３は、ＯＲ回路１９へ入力される。
【００３９】ＯＲ回路１９の前記した他方の入力信号である実動作モード信号１３は、ユーザプログラム が起動する時の信号であり、このコピーモード時にはＬｏｗ信号である。よって、ＯＲ回路１９から出力されるＬｏｗ信号がトライステートバッファ２０のコントロールゲートへ入力されてフローティング状態になり、かつ、制御装置１内にあるアルゴリズム 内蔵 手段２内で実行中のプログラム がコピーモード動作に対する待機状態でないので、内蔵 フラッシュメモリ２１のデータをコピーモードボードから読み出すことが不可能となると同時にコピーモードボードの制御そのものも受け付けなくなってしまう。
【００４０】残り、オンボードモード時も前記したＰＲＯＭモード、コピーモード時と同様に、最終のデータ書き込みサイクル期間、制御装置１よりオンボードモード書き込み終了信号９にライト信号２８パルス出力に対し、セットアップ、ホールド期間を保持してＨｉｇｈを出力させる。以後、前記したモードと同様に最終のデータ書き込みサイクル期間だけ、トライステートバッファ２２のコントロールゲートが開き、内蔵 フラッシュメモリ２１からのデータをセキュリティ専用フラッシュメモリ１４に、セキュリティコードとして書き込み、オンボードモード書き込み終了信号９と共に設定される。

【００４１】そして、セキュリティ専用フラッシュメモリ１４はオンボードモードに対するセキュリティが設定されたと認識し、オンボードモードセキュリティ信号１７を出力し、この信号を受けて、制御装置１内にあるアルゴリズム 内蔵 手段２内のプログラム で強制的に無限ループルーチンへ起動を掛ける。この起動により制御装置１より無限ループフラグ信号１３にＬｏｗが出力される。

【００４２】このＬｏｗ信号１３はＯＲ回路１９へ入力され、残りの入力信号の実動作モード信号１３もオンボードモード時にはＬｏｗ信号であるので、ＯＲ回路１９はＬｏｗ信号を出力し、トライステートバッファ２０はフローティング状態になる。制御装置１内にあるアルゴリズム 内蔵 手段２内で実行中のプログラム がオンボードモード動作に対する待機状態でないので、内蔵 フラッシュメモリ２１のデータをオンボードモードボードから読み出すことが不可能となると同時にオンボードモードの制御そのものも受け付けなくなる。

【００４３】以上説明したような各モードによるメモリデータ内容の読み出し禁止状態を唯一解除する動作として、テストモード信号３１とセキュリティコード入力信号３２を特定端子に割り当て必要信号を入力するテストモードが用意されいる。

【００４４】ここでセキュリティコード入力信号３２には、セキュリティ専用フラッシュメモリ１４へ書き込んだ最終データ（例えば、８ビットデータ長であれば、８本の入力端子の設定）を設定する必要がある。この場合、データ入力を行ったオペレータは最終データを理解しているこからセキュリティコード入力信号３２への入力をミスなく行うことができが、他人は最終データを知り得ないことからセキュリティコードとして機能する。

【００４５】この様に入力条件が満たされたテストモード状態は、アルゴリズム 内蔵 手段２内のプログラム でセキュリティ専用フラッシュメモリ記憶手段１４に設定されているデータコード３３と該当するテストモード条件の一致が認識されたときのみ、テストモード一致信号１１にＨｉｇｈを出力する。

【００４６】このテストモード一致信号１１で、セキュリティ専用フラッシュメモリ記憶手段１４の一致信号１８に対するビットがＨｉｇｈにセットされる。一致信号１８にＨｉｇｈが出力されることで、アルゴリズム 内蔵 手段２内のプログラム はこの一致信号１８を認識して各モード時における無限ループルーチンの制御を各モードに該当するセキュリティの設定されていないデータ書き込み動作、消去動作、及び読み出し動作のいずれかに相当するルーチン待ちの状態へ移行させる。この動作と連動して無限ループフラグ信号１３は、ＬｏｗからＨｉｇｈ信号となることで、ＯＲ回路１９による出力信号はＨｉｇｈとなり、トライステートバッファ２０のコントロールゲートがアクティブとなるので内蔵 メモリデータの内容が読み出し可能となる。

【００４７】また、前述の３つの動作モードにおいて、新たに内蔵 フラッシュメモリ２１に書き込みあるいは消去を行うことも可能となり、内蔵 フラッシュメモリ２１に格納されているプログラム やデータのメンテナンスが可能となる。

【００４８】尚、このテストモードによる読み出しを前述の３つのモードと同様に読み出し禁止とするためには、該当するテストモード状態とセキュリティコード入力信号３２をフラッシュメモリの最終データと一致しない信号を入力することで、各モード時のセキュリティ動作で説明したプロセス、すなわちを無限ループフラグ信号１３をアクティブにすることで同様なセキュリティが可能となる。

【００４９】なお、前記の実施形態では本発明の好適例を説明したが、本発明はこれに限定されないことはもちろんである。例えば、本発明におけるセキュリティコードは、従来のように予めセキュリティコードを入力するのではなく、入力データから所定規則に基づいてセキュリティコードが自動的に作成されるものであればよく、本実施形態では最終のデータをセキュリティコードとして用いる場合を説明したが、例えば、入力データの最初のデータや、所定ルールに基づくデータを用いてもよく、適宜回路を変更することで同様の作用効果を発揮する。また、本実施形態では、説明の便宜上１チップマイクロコンピュータを例に発明を説明したが、１チップに限定するものでないことは言うまでもない。

【００５０】

【発明の効果】以上説明した通り、本発明の第１、２の要旨によれば、予めセキュリティコードやパスワードを設定することなく自動的に内蔵 フラッシュメモリの読み出し等を禁止でき、かつ、改めてセキュリティコードを用意する必要もなくなるのでセキュリティコード管理も不要となり、簡単に不揮発性メモリ内のデータの秘密保持が可能となった。

【００５１】要旨３によれば、アクセス禁止手段がアルゴリズム 内蔵 手段に格納されたアルゴリズム で無限ループを実行することで、アクセス待ち状態が無くなり、見かけ上デバイス自体が内蔵 メモリをアクセスできない故障あるいは不良の状態と同等となるため、実質的に他者によるメモリデータの読み出しは困難でありメモリ内容のセキュリティーが保たれる。

【００５２】要旨４によれば、セキュリティコードは所定ルールに基づくものであり、データを書き込んだ者は知り得ることから、不揮発性メモリ内のデータの修正等を行なう場合にはセキュリティコードと一致するデータを外部より入力することにより、プログラム のバグ発生に伴うメンテナンスを可能とできた。

【００５３】要旨５によれば、不揮発性メモリ内のデータ、例えばプログラム のバグ発生に伴うメンテナンス

後、再度セキュリティを簡単にかけることも可能となるので、セキュリティとプログラム やバグ等によるメンテナンス等が確実に行える。

【００５４】要旨６によれば、セキュリティコードを不揮発性メモリへ書き込まれる最終データとすることで、セキュリティコード等の設定が簡単な回路により実現することができる。

【図面の簡単な説明】

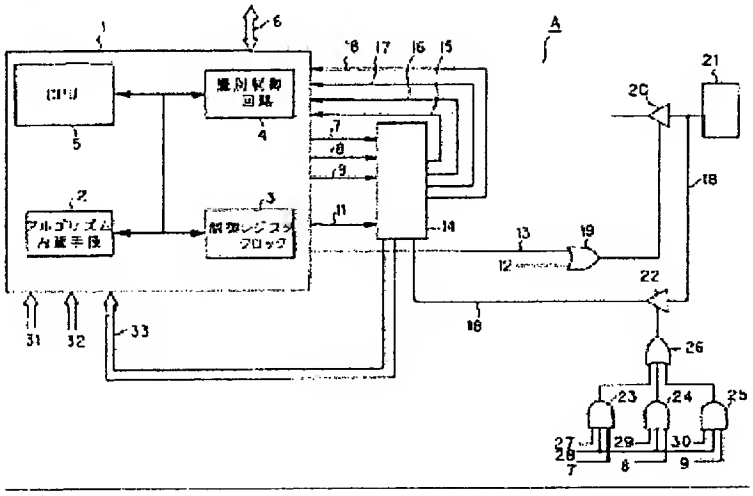
【図１】本発明の実施形態に係る不揮発性メモリ内蔵 １チップマイクロコンピュータの概略的ブロック図である。

【図２】従来の不揮発性メモリ内蔵 １チップマイクロコンピュータの作用的ブロックである。

【符号の説明】

Ａ　１チップマイクロコンピュータ
１　制御装置
２　アルゴリズム 内蔵 手段
１４　セキュリティ専用フラッシュメモリ
１９　ＯＲ回路
２０　トライステートバッファ
２１　内蔵 フラッシュメモリ

【図１】



【図２】